ZETLIN & DE CHIARA LLP

Put Your Records On by Patricia Harris, September 2008

Many businesses are renewing their focus on records management and retention policies for a number of reasons. First, increased reliance on email has created a new and significant category of extemporaneous communication that must be monitored, managed and stored. Second, the portability of electronic data and ease of duplication has created a loss of control that businesses historically exercised over their own records and work-product. Electronic records can be easily manipulated and are open to a multitude of internal and external threats. Third, the cost of storing hard documents has become significant to many businesses, thereby causing an increased reliance on electronic or virtual storage. Finally, legal guidelines pertaining to document management in the face of litigation are quickly evolving and a wrong step with respect to document preservation can have serious consequences. A comprehensive records management policy can and should address many of these issues.

OVERALL RECORDKEEPING

Certain business records, such as organizational documentation, financial records, licenses, trademarks, patentsand copyrights, should be retained permanently. Many other types of businesses records must be preserved for a specific period of time as a matter of law. Often, records such as tax records will be retained in conjunction with a specific statute of limitations period. These periods are often set by individual state law and it is prudent to consult an attorney or accountant to review

specific jurisdictional rules. The business should have a procedure for the storage and eventual destruction of personnel records (including employee files, payroll records and workers' compensation claims), insurance records, vendor contracts, advertising materials and general correspondence. It is important to pay particular attention to the storage and security of personnel records; businesses may find themselves governed by the regulations and subject to the penalty provisions of such far-flung legislation as the Fair Credit Reporting Act, HIPPA and numerous state privacy laws.

MANAGEMENT OF EMAIL

There is no other way to say it - email is dangerous. Most people treat email as an alternative to speaking andwe often find such correspondence to be casual, off-the-cuff, emotional. It must be remembered and it must be drilled into employees, however, that email is anything but casual. Email is written documentation, carrying the same weight in a court of law or in any dispute, as a formal business letter, plan or record. Moreover,there is no opportunity for revision or second thoughts once that "send" button is hit. Email can be forwarded to anyone without the sender's permission or knowledge. Finally, all email is date and time-stamped. The negative implications of this "email culture" run the gamut from embarrassment to misunderstandings togrounds for litigation.

The business should implement a written policy regarding the proper use of electronic communication. Employees should acknowledge in writing that they will be abide by the policy. Email usage should be monitored periodically to ensure compliance with the policy.

In addition to policies regarding email communication, the business must develop procedures relating to itsstorage. Segregate and preserve email as required. First and foremost, substantive emails should be saved as part of specific project files; in this way, should the business have to produce such communications in connectionwith an investigation or litigation, the files will be easy to access and the chance of producing irrelevant and/or confidential information will be minimized. Emails stored within the general email system, i.e., those notspecifically filed and preserved, should be deleted regularly.

THE DATA LIFE CYCLE

In the context of records management, there are five important steps in the life of a document: (i) acquisition,(ii) storage, (iii) usage, (iv) distribution and sharing, and (v) archiving or destruction. The business should develop a policy and procedure for, and designate the technology involved in, each of these stages. For example, in connection with acquisition, are files acquired from third parties in a way that may threaten the integrity of the business' IT system? In terms of storage, the length of retention should be prescribed. Who has accessto what records and what methods of security will

be used to protect the firm's records? Destruction policies and methods should be established. Most importantly, the firm's policies must be communicated to all involved.

The records destruction policy should be as important to a business as is its retention policy. Although a firm cannot fully control the destiny and destruction of its records, particularly with respect to emails or other documents shared with or provided to third parties, an ongoing destruction program allows for greater internal document control, and may also benefit the business and minimize the burdens of extraordinary document production should it be asked to produce documents in a litigation context. The policy should define destruction milestones, e.g., during the course of a project and at project close-out. Establish policies pertaining to redundant electronic backup systems as well as records "outside" of the business' control, such as records storedon PDA's, home computers, in storage facilities and in employees' garages. A comprehensive destruction policy will address paper as well as electronic documents. Finally, minimize individual discretion. The policy should designate one executive-level decision-maker who can make thoughtful and consistent decisions in the event of questions or regarding which records should stay and which should go.

FOR A/E FIRMS — MANAGEMENT OF PROJECT DATA

The lifeblood for the A/E business is project data. It is crucial to define project data so that all employees know what documentation to retain and what should be handled with care. Required document retention periods for project data may come from a number of sources. First, the firm should look to any requirements, particularly arising out of the relevant statutes of limitation and repose, in the jurisdiction in which the project is located. Second, contract documents in connection with particular projects may contain records retention directives. Finally, A/E firms may be subject to other jurisdictional rules such as Part 29.3 (4) of the New York Board ofRegents Rules, which states that unprofessional conduct includes:

Failure by a licensee to maintain for at least six years all preliminary and final plans, documents, computations, records, and professional evaluations prepared by the licensee, or the licensee's employeesrelating to work to which the licensee has affixed his seal and signature.

LITIGATION PROTOCOL

One rapidly-changing area of law relates to the preservation of records, specifically electronic records, in theface of litigation. Negligent spoliation of evidence has led to fines and/or the dismissal of legal claims anddefenses, while intentional spoliation, in some very public cases, has led to prison. Once the firm is served with a subpoena or request for documents, or an employee becomes aware of a governmental investigation or audit, or litigation against the firm is commenced, all relevant documents must be preserved. Normal document destruction policies or any other manipulation of

relevant records must cease.

The first step in records preservation when an investigation or litigation arises is to put together an internal preservation team. The team should be composed of personnel from IT, records management, system security and human resources. While it may seem incongruous to include an HR team member, HR people are often the first to be aware of a departing employee and, in such position, can inform the team to make special effortsto preserve or retrieve information from such individuals. It is fine, and from a lawyer's perspective, encouraged that the business be overly broad in preserving documents when it becomes aware of a litigation or investigation; preservation parameters can and should be defined and narrowed with the assistance of legal counsel.

Businesses have a duty to preserve what is known or reasonably should have known is relevant to the action, is reasonably calculated to lead to the discovery of admissible evidence or is reasonably likely to be requested during discovery. Again, it is imperative that the firm have a written "litigation hold" policy. Providing such a policy is in place and consistently implemented, it is unlikely a court will require a firm to take extraordinary steps to preserve or retrieve its electronic records.

Technology is a great thing. It has allowed many businesses to advance and grow and produce excellent work. With that advancement and growth and work come more records, more documents, and more avenues of communication and options for storage. Businesses must keep up. It is important to review issues and to develop policies associated with records management on a regular basis. In the immortal words of Yogi Berra, "I always thought that record would stand until it was broken."